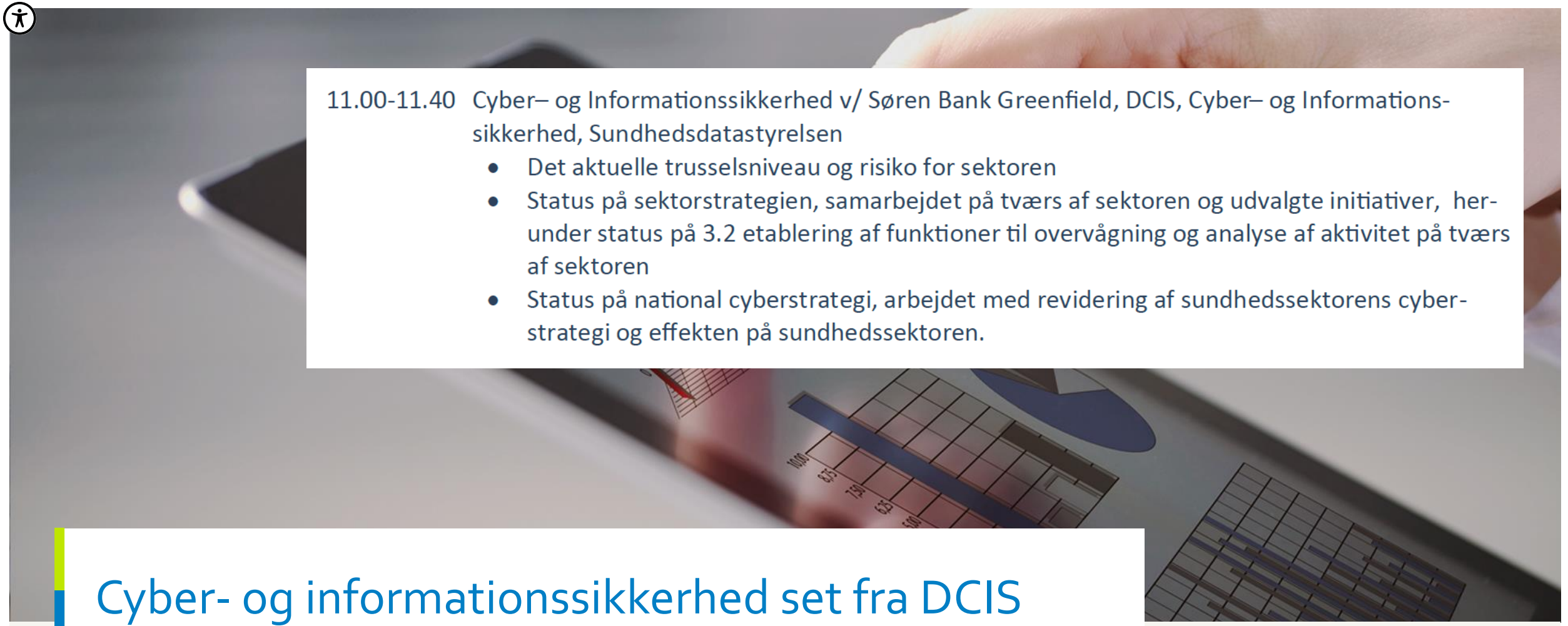


11.00-11.40 Cyber– og Informationssikkerhed v/ Søren Bank Greenfield, DCIS, Cyber– og Informations-sikkerhed, Sundhedsdatastyrelsen

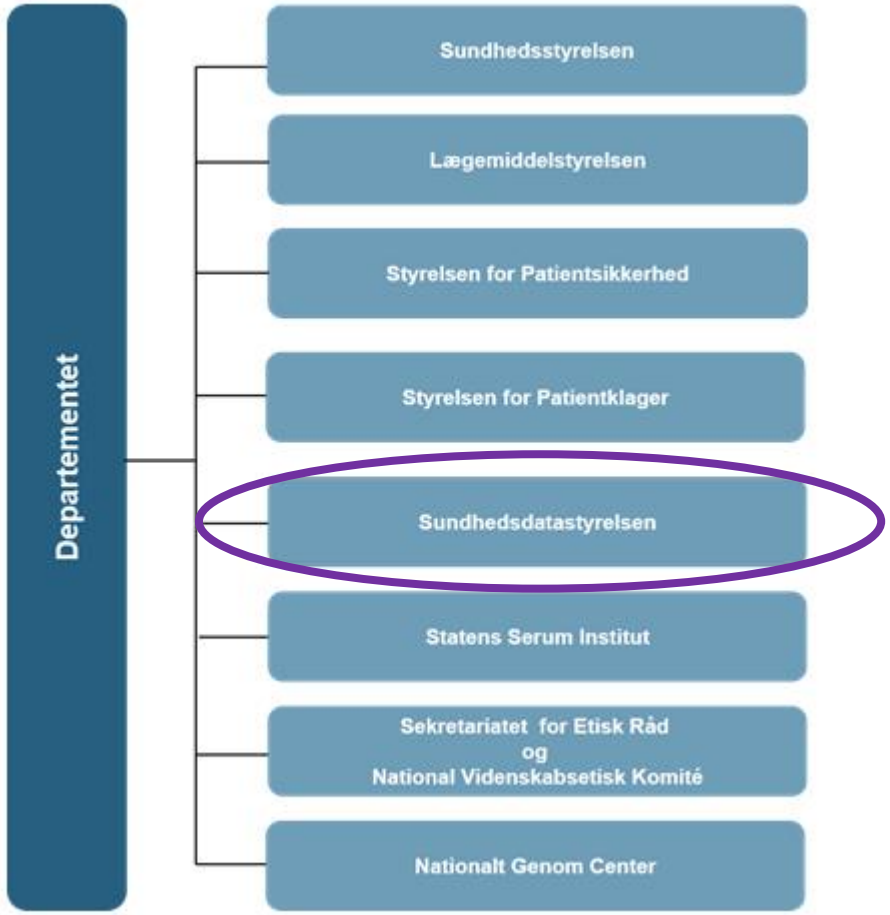
- Det aktuelle trusselsniveau og risiko for sektoren
- Status på sektorstrategien, samarbejdet på tværs af sektoren og udvalgte initiativer, her-under status på 3.2 etablering af funktioner til overvågning og analyse af aktivitet på tværs af sektoren
- Status på national cyberstrategi, arbejdet med revidering af sundhedssektorens cyber-strategi og effekten på sundhedssektoren.

Cyber- og informationssikkerhed set fra DCIS sund

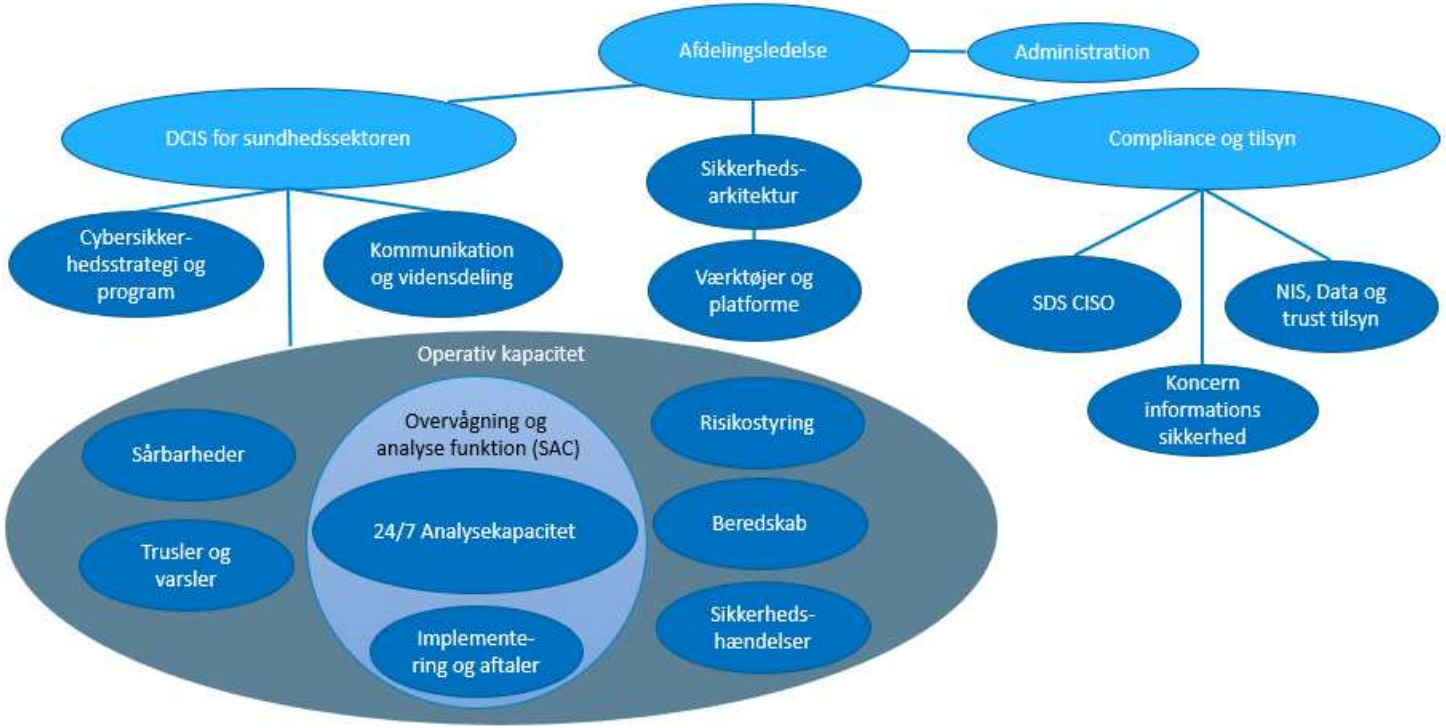
V/ Søren Bank Greenfield
Afdelingschef i SDS Cyber og –informationssikkerhed

SUNDHEDSDATA-STYRELSEN

Sundhedsministeriet



Afdelingen har til opgave at facilitere og koordinere den fælles indsats for at **styrke og øge** kapabiliteten og kapaciteten inden for cyber- og informationssikkerhed i Sundhedsdatastyrelsen, Sundhedsministeriet og **på tværs af sundhedssektoren.**



SUNDHEDSDATA-STYRELSEN

Det aktuelle trusselsbillede

Også set i forhold til krigen i Ukraine

SUNDHEDSDATA-
STYRELSEN

SUNDHEDSDATA-STYRELSEN

TLP:WHITE

SUNDHEDSDATA-STYRELSEN

Varsler & hændelser i sundhedssektoren

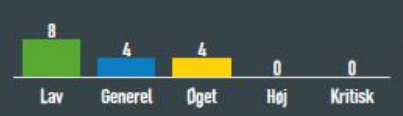
2. Kvartal 2021

Generel

Udvalgte varsler

- DNS sårbarheder
- FluBot smishing
- Sårbarhed i Kerberos

Antal udsendte varsler



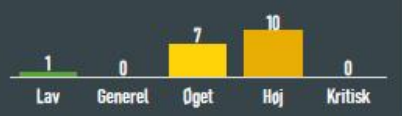
3. Kvartal 2021

Generel

Udvalgte varsler

- Kritisk sårbarhed i FortiWeb OS
- Aktiv udnyttelse af ProxyShell sårbarheder
- Sårbarheder i Atlassain Confluence
- Sårbarheder i Palo Alto produkter

Antal udsendte varsler



4. Kvartal 2021

Øget

Udvalgte varsler

- Kritisk sårbarhed i Apache Log4j kodebibliotek
- Citrix ADC, Citrix Gateway og Citrix SD-WAN WANOP
- Zero-day i Windows installer (MSI)
- Multiple Vulnerabilities in Apache HTTP Server Affecting Cisco Products

Antal udsendte varsler

1. Kvartal 2022

Øget

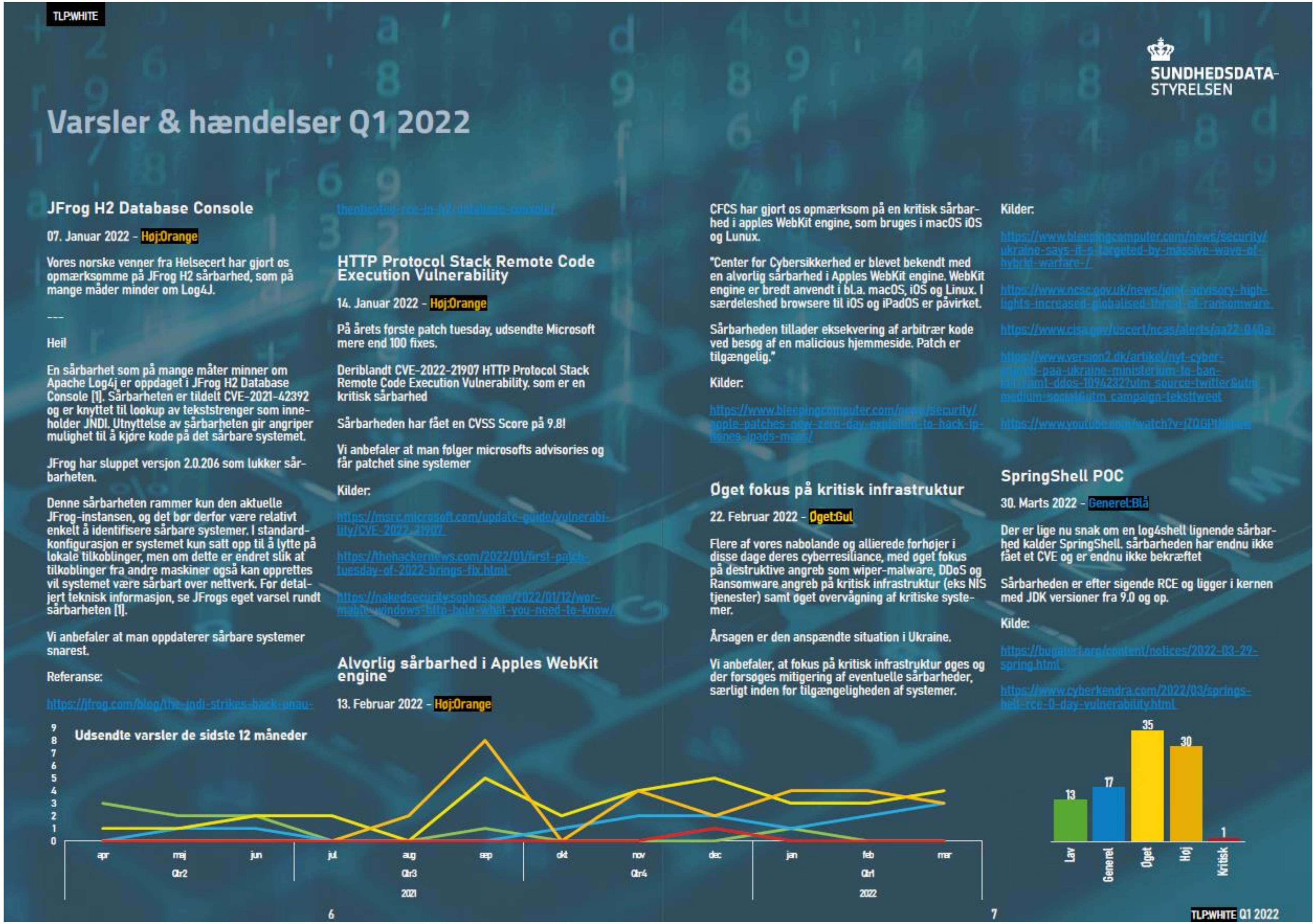
Udvalgte varsler

- Destruktive cyberangreb observeret mod ukrainske organisationer
- Zero-day fix til apple enheder
- Zero-day i Google Chrome browser
- Øget fokus på kritisk infrastruktur
- 2 Zero-days i Mozilla Firefox
- Sårbarhed i Infusionspumper

Antal udsendte varsler

cybervejrudsigt_q1_2022.pdf (sundhedsdatastyrelsen.dk)

SUNDHEDSDATA-STYRELSEN



TLP:WHITE

SUNDHEDSDATA-STYRELSEN

Varsler & hændelser Q1 2022

JFrog H2 Database Console

07. Januar 2022 - Høj:Orange

Vores norske venner fra Helsecert har gjort os opmærksomme på JFrog H2 sårbarhed, som på mange måder minder om Log4J.

Hei!

En sårbarhet som på mange måter minner om Apache Log4j er oppdaget i JFrog H2 Database Console [1]. Sårbarheten er tildelt CVE-2021-42392 og er knyttet til lookup av tekststrenger som inneholder JNDI. Utnyttelse av sårbarheten gir angriper mulighet til å kjøre kode på det sårbare systemet.

JFrog har sluppet versjon 2.0.206 som lukker sårbarheten.

Denne sårbarheten rammer kun den aktuelle JFrog-instansen, og det bør derfor være relativt enkelt å identifisere sårbare systemer. I standardkonfigurasjon er systemet kun satt opp til å lytte på lokale tilkoblinger, men om dette er endret slik at tilkoblinger fra andre maskiner også kan opprettes vil systemet være sårbart over nettverk. For detaljert teknisk informasjon, se JFrogs eget varsel rundt sårbarheten [1].

Vi anbefaler at man oppdaterer sårbare systemer snarest.

Referanse:

https://jfrog.com/blog/the-jndi-strikes-back-unauthenticated-rce-in-h2-database-console/

HTTP Protocol Stack Remote Code Execution Vulnerability

14. Januar 2022 - Høj:Orange

På årets første patch tuesday, udsendte Microsoft mere end 100 fixes.

Deriblandt CVE-2022-21907 HTTP Protocol Stack Remote Code Execution Vulnerability. som er en kritisk sårbarhed

Sårbarheden har fået en CVSS Score på 9.8!

Vi anbefaler at man følger microsofts advisories og får patchet sine systemer

Kilder:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907

https://thehackernews.com/2022/01/first-patch-tuesday-of-2022-brings-fix.html

https://nakedsecurity.sophos.com/2022/01/12/wormable-windows-http-hole-what-you-need-to-know/

Alvorlig sårbarhed i Apples WebKit engine

13. Februar 2022 - Høj:Orange

CFCS har gjort os opmærksom på en kritisk sårbarhed i apples WebKit engine, som bruges i macOS iOS og Lunux.

"Center for Cybersikkerhed er blevet bekendt med en alvorlig sårbarhed i Apples WebKit engine. WebKit engine er bredt anvendt i bl.a. macOS, iOS og Linux. I særdeleshed browsere til iOS og iPadOS er påvirket.

Sårbarheden tillader eksekvering af arbitrær kode ved besøg af en malicious hjemmeside. Patch er tilgængelig."

Kilder:

https://www.bleepingcomputer.com/news/security/apple-patches-new-zero-day-exploited-to-hack-iphones-ipads-macs/

Øget fokus på kritisk infrastruktur

22. Februar 2022 - Øget:Gul

Flere af vores nabolande og allierede forhøjer i disse dage deres cyberresiliance, med øget fokus på destruktive angreb som wiper-malware, DDoS og Ransomware angreb på kritisk infrastruktur (eks NIS tjenester) samt øget overvågning af kritiske systemer.

Årsagen er den anspændte situation i Ukraine.

Vi anbefaler, at fokus på kritisk infrastruktur øges og der forsøges mitigering af eventuelle sårbarheder, særligt inden for tilgængeligheden af systemer.

Kilder:

https://www.bleepingcomputer.com/news/security/ukraine-says-it-s-targeted-by-massive-wave-of-hybrid-warfare-/

https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware

https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

https://www.version2.dk/artikel/nyt-cyberangreb-paa-ukraine-ministerium-to-banker-ramt-ddos-1094232?utm_source=twitter&utm_medium=social&utm_campaign=tekstitweet

https://www.youtube.com/watch?v=jZOGPtNgpw

SpringShell POC

30. Marts 2022 - Generel:Blå

Der er lige nu snak om en log4shell lignende sårbarhed kalder SpringShell. sårbarheden har endnu ikke fået et CVE og er endnu ikke bekræftet

Sårbarheden er efter sigende RCE og ligger i kernen med JDK versioner fra 9.0 og op.

Kilde:

https://bugalert.org/content/notices/2022-03-29-spring.html

https://www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html

[cybervejrudsigt_q1_2022.pdf (sundhedsdatastyrelsen.dk)](cybervejrudsigt_q1_2022.pdf)

Risiko i internationalt perspektiv

- Dette kan ændre sig MEGET hurtigt – dag til dag!
- Så det anbefales at man gør sig parat man kan og så robust som muligt.

Hovedvurdering

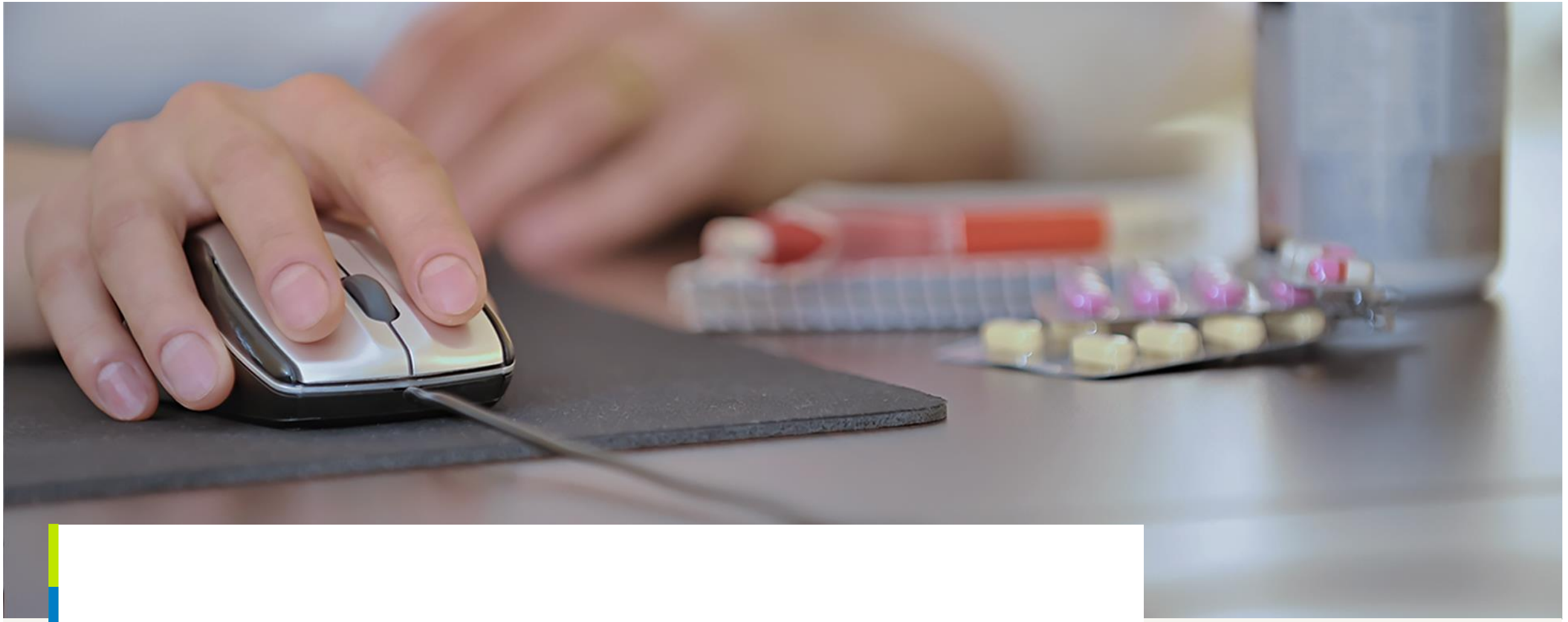
- Truslen fra cyberkriminalitet er **MEGET HØJ**. Alle danske myndigheder, virksomheder og borgere er udsat for en vedvarende og aktiv trussel fra cyberkriminelle. Truslen underbygges af de cyberkriminelles evne til at udvikle og omstille sig til nye virkeligheder samt det specialiserede samarbejde, der foregår på lukkede internetfora.

- Truslen fra cyberspionage er **MEGET HØJ**. CFCS vurderer, at fremmede stater kan og vil forsøge på at stjæle værdifuld information fra Danmark. Særligt interessante mål på det udenrigs- og sikkerhedspolitiske område er udsat for en vedvarende interesse fra statslige aktører. Konkrete hændelser og løbende angrebsforsøg understreger gang på gang denne vurdering.

- CFCS vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder er **LAV**. Flere stater har kapaciteten til at udføre destruktive angreb, men det er mindre sandsynligt, at de aktuelt har intention om at udføre den type angreb mod danske mål.

- Truslen fra cyberaktivisme e[Mellem]…ge protester, der har præget 2020, har ikke ført til en stigning i antallet af cyberaktivistiske angreb på verdensplan. Antallet af angreb ligger således på niveau med de seneste år.

- Truslen fra cyberterror er **INGEN**. Alvorlige cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt begrænset.



Effekten af den ny national strategi og NIS 2.0

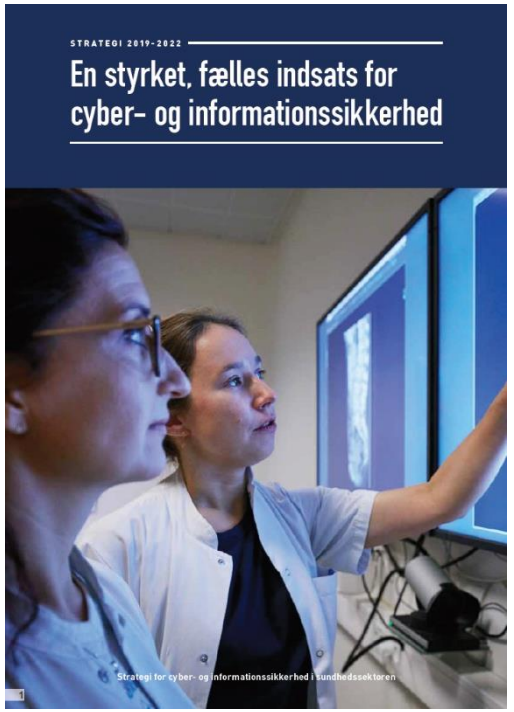
+ Plan for revidering af sundhedssektorens cyber- og informationssikkerhedsstrategi

SUNDHEDSDATA-
STYRELSEN

Strategisk niveau

Den nationale strategi for cyber- og informationssikkerhed fra maj 2022-2024

Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022

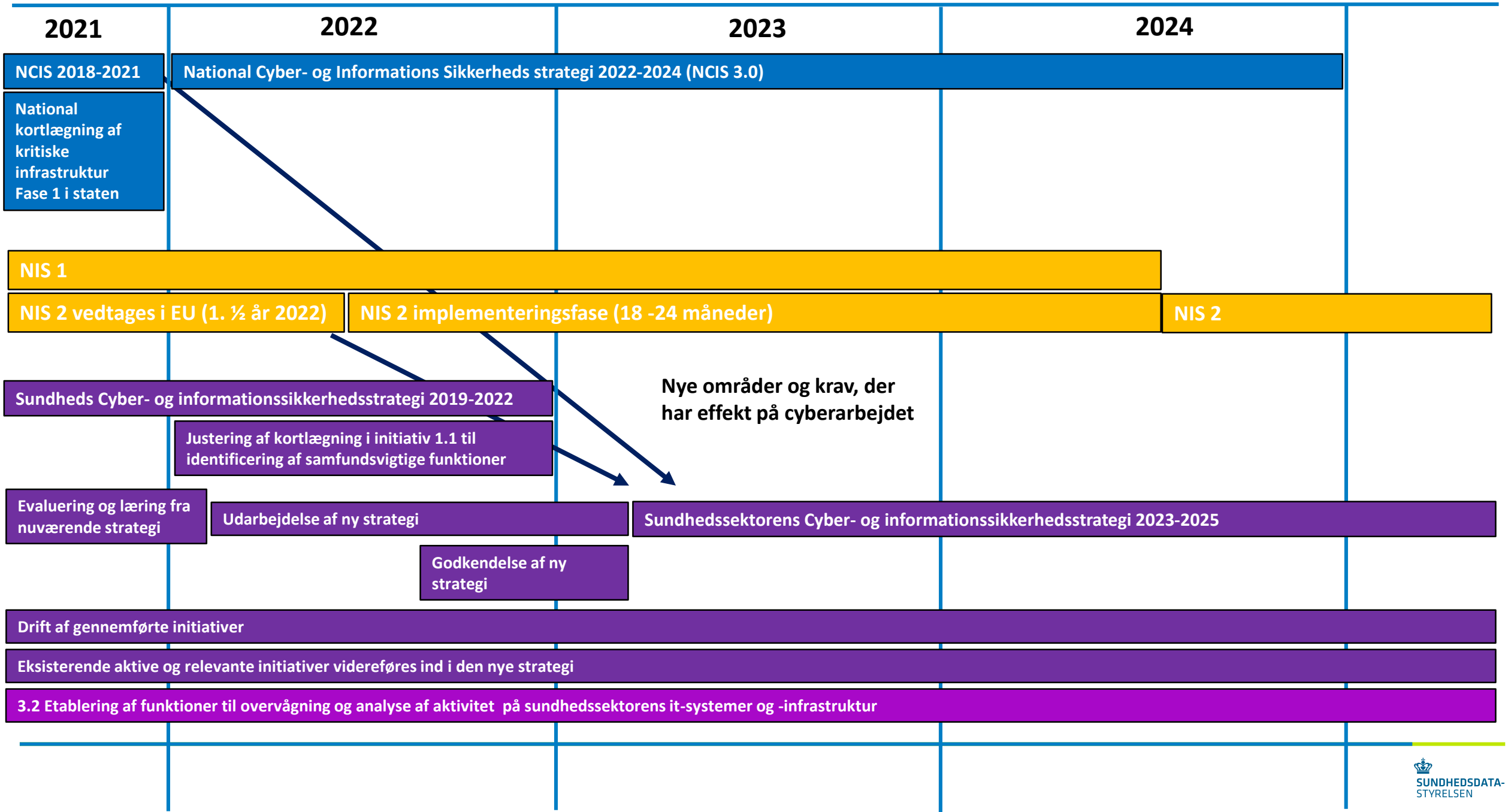


Ny strategi 1/1 2023

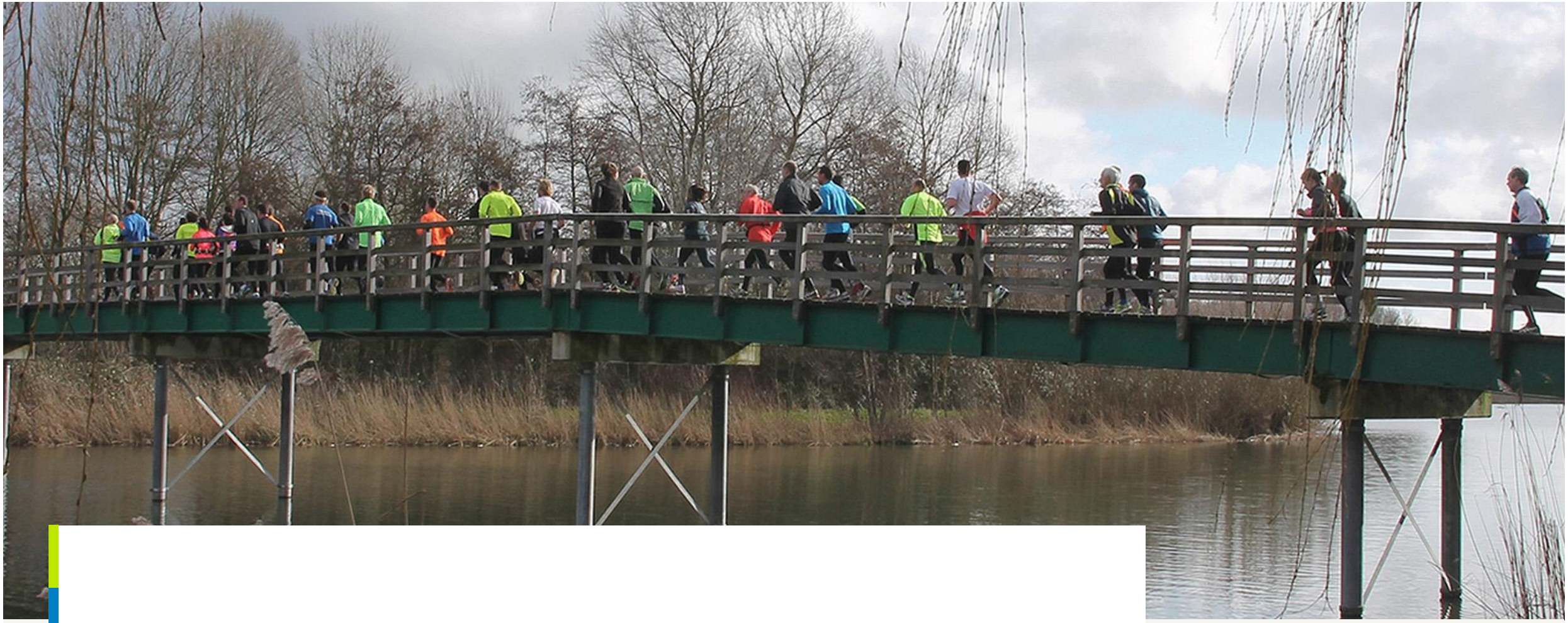
https://digst.dk/strategier/cyber-og-informationssikkerhed/
https://sundhedsdatastyrelsen.dk/da/strategier-og-projekter/cyberstrategi

SUNDHEDSDATA-STYRELSEN

Strategisk arbejde med cyber- og informationssikkerhed



SUNDHEDSDATA-STYRELSEN



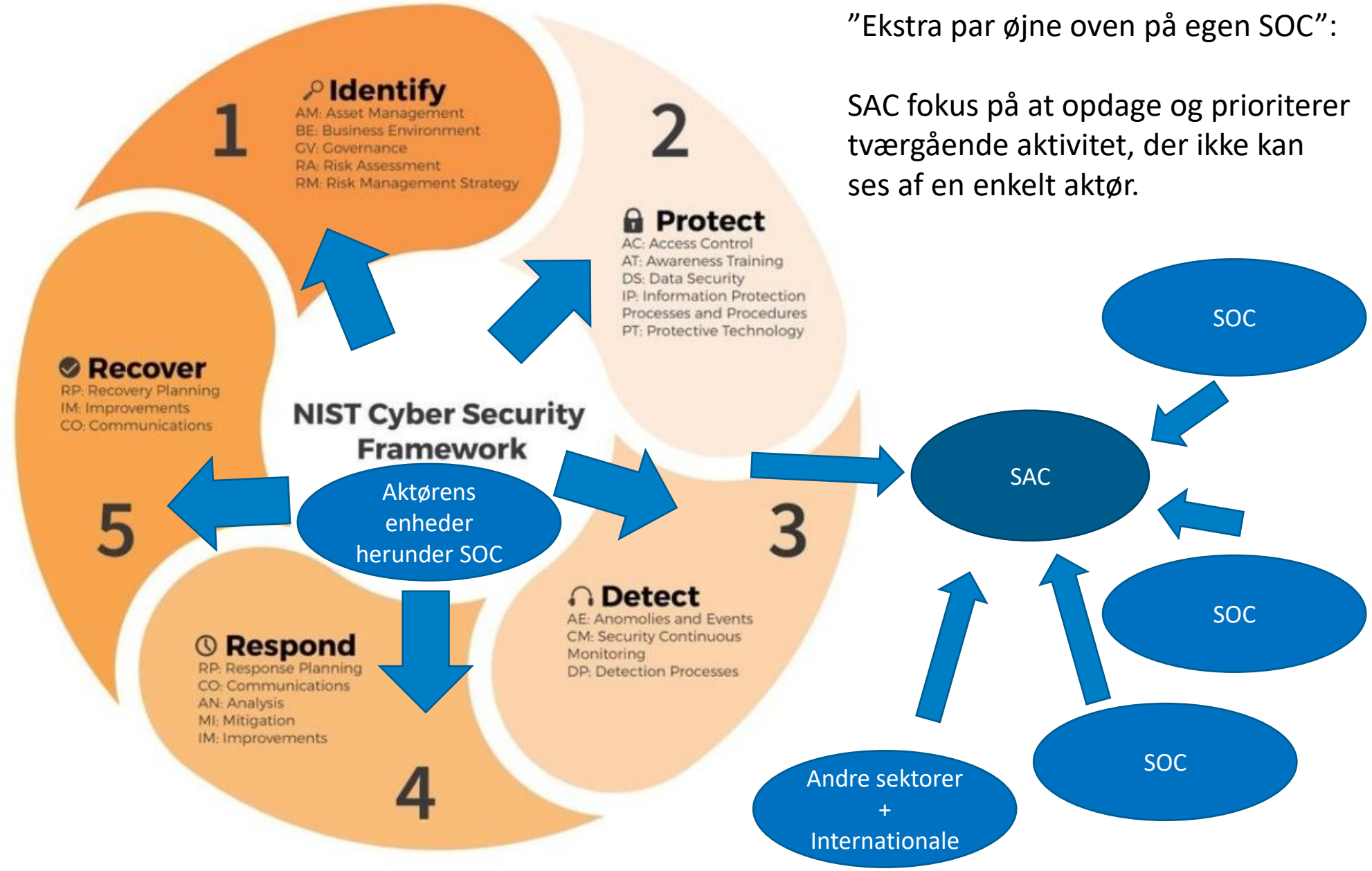
Specifik status på initiativ 3.2

Etablering af funktioner til overvågning og analyse af aktivitet på sundhedssektorens it-systemer og -infrastruktur

SUNDHEDSDATA-
STYRELSEN

”Ekstra par øjne oven på egen SOC”:

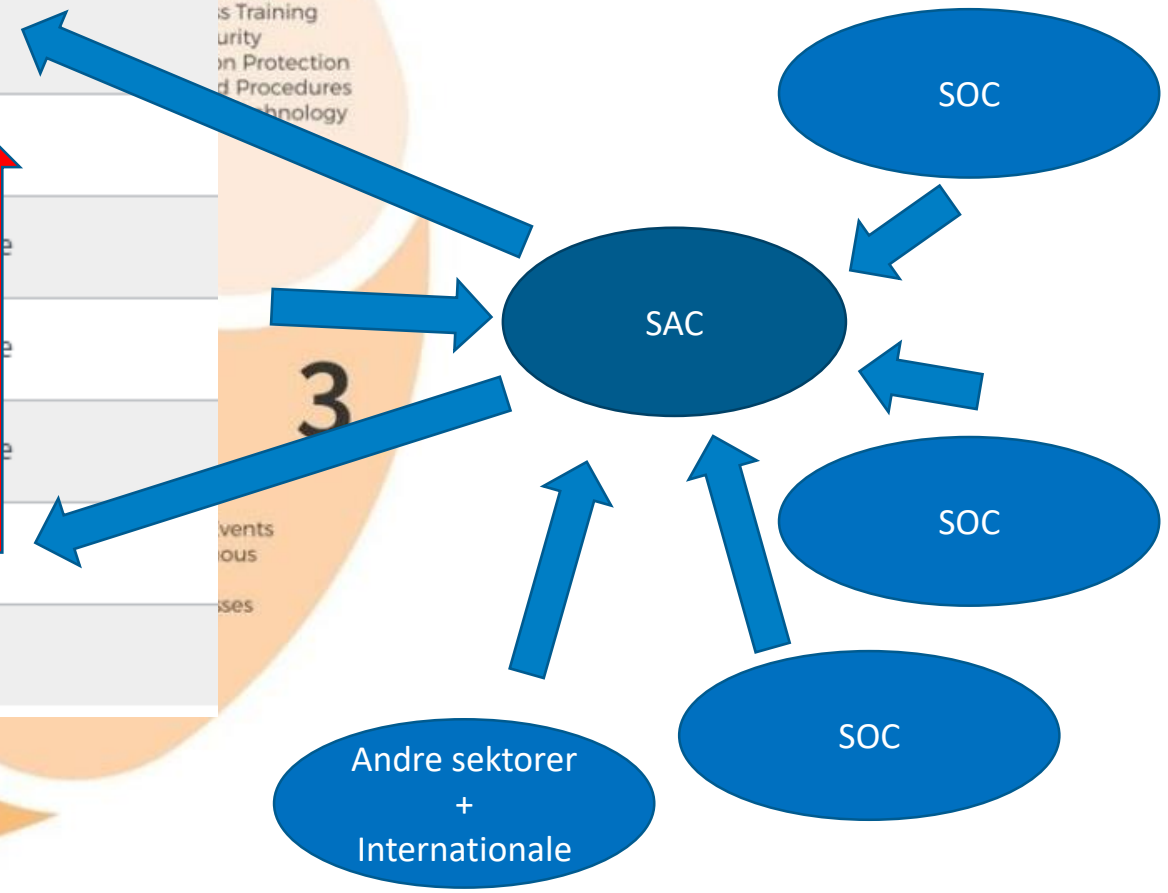
SAC fokus på at opdage og prioriterer tværgående aktivitet, der ikke kan ses af en enkelt aktør.



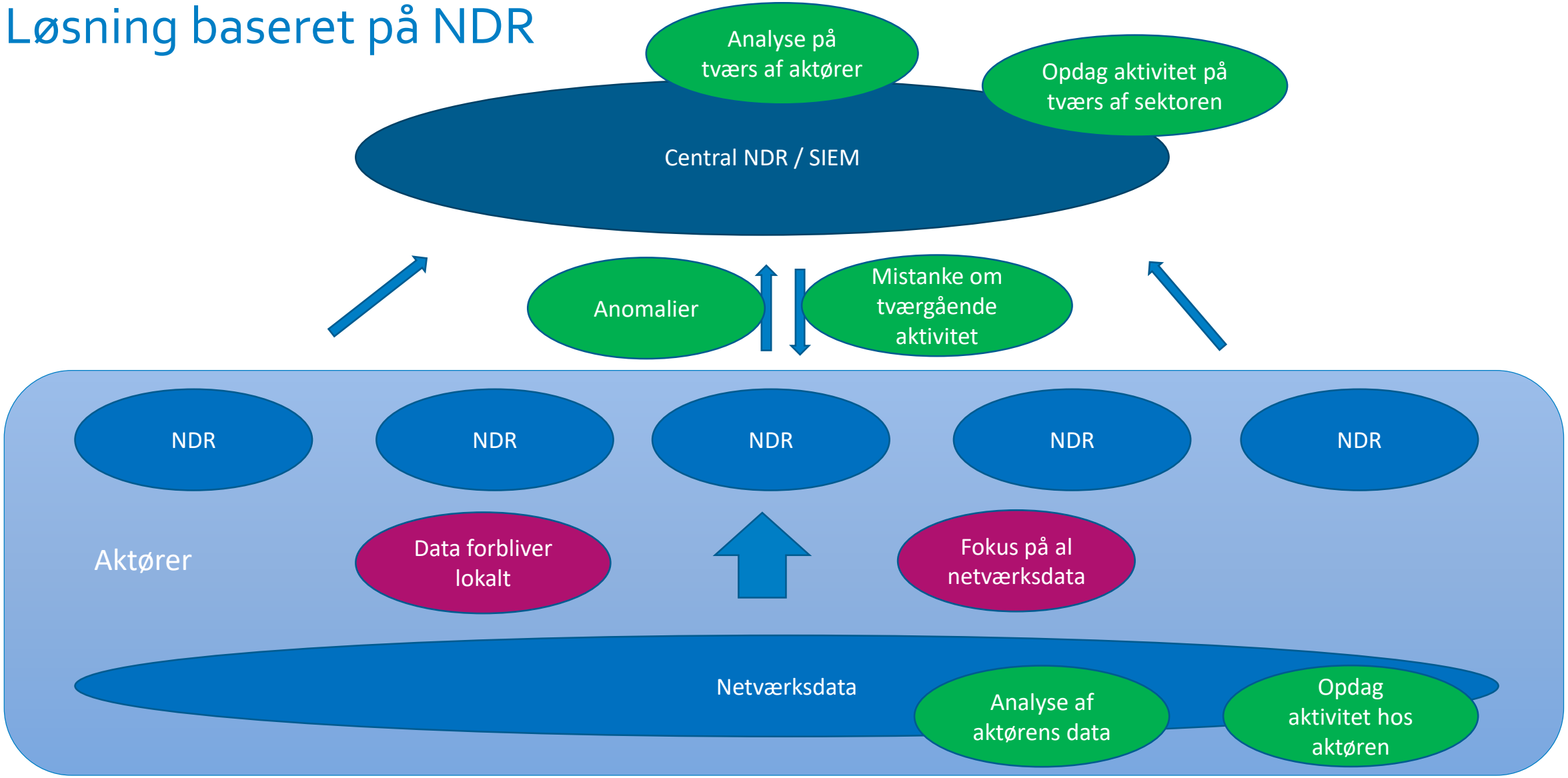
”Ekstra par øjne oven på egen SOC”:

SAC fokus på at opdage og prioriterer tværgående aktivitet, der ikke kan ses af en enkelt aktør.

Impact	Urgency	Priority ▲
Search	Search	Search
1 - High	1 - High	1 - Critical
2 - Medium	1 - High	2 - High
1 - High	2 - Medium	2 - High
3 - Low	1 - High	3 - Mode
2 - Medium	2 - Medium	3 - Mode
1 - High	3 - Low	3 - Mode
3 - Low	2 - Medium	4 - Low
2 - Medium	3 - Low	4 - Low



Løsning baseret på NDR



National

MISP Threat Sharing

International

norskhelsenett

H-ISAC HEALTH - ISAC

DCIS-SUND – Sundhedsdatastyrelsen

Triagering

Triagering

MISP Threat Sharing

TELEDCIS

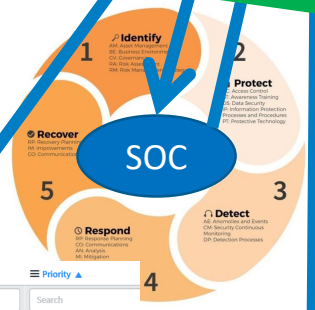
SFS-DCIS

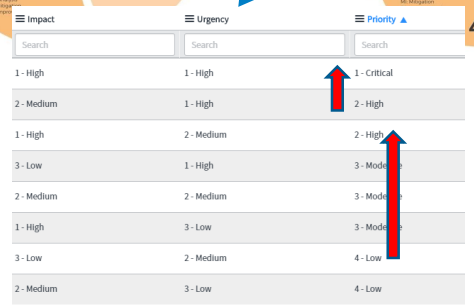
FINANSTILSYNET

”Ekstra par øjne oven på egen SOC”
”Giver tilbage til sektoren”
”Sektor situationsoverblik”
”Udbyder værktøjer til sektoren”

SAC

Operativt samarbejde

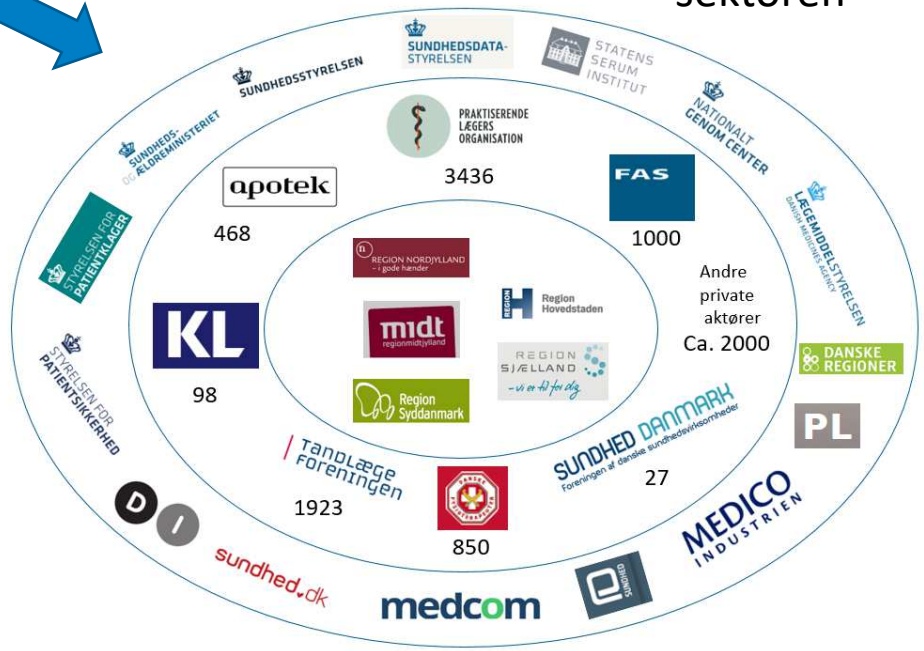




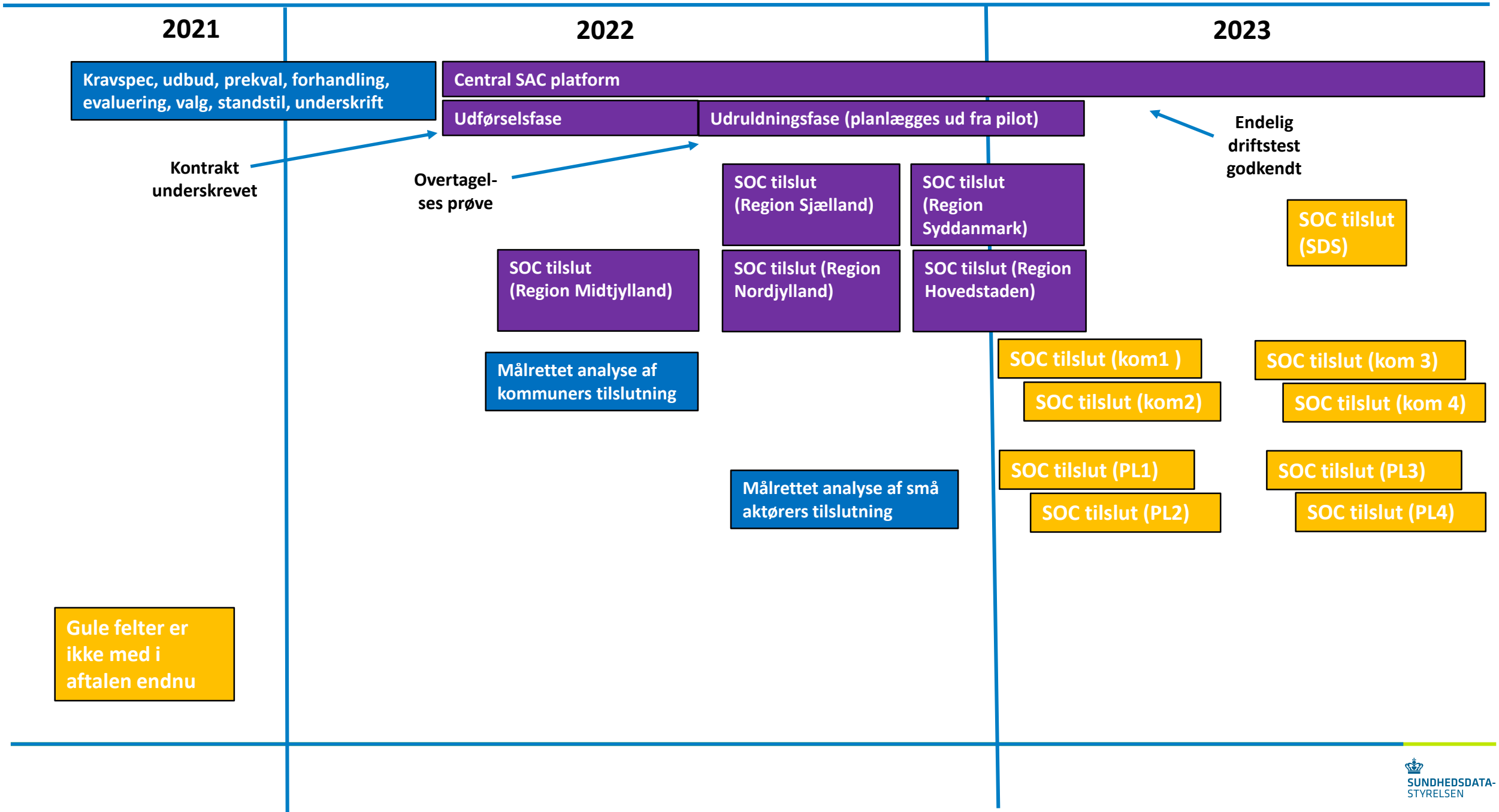
Mulighed for automatisk beskyttelse ud fra IOC’er”

Fuldt operative SOC

Resten af sektoren



Funktioner til Overvågning- og Analyse kapacitet for sundhedssektoren



SUNDHEDSDATA-STYRELSEN

Opsamling ☺

SUNDHEDSDATA-
STYRELSEN

Opsamling

- Der er er forøget risiko fra cybercriminelle, både direkte og ”spill over” fra cyberkrigen omkring Ukraine.
- Vi fortsætter med øget opmærksomhed og brief 1 gang om måneden.
- Den nationale strategi forsøges understøttet gennem sundhedssektorens egen strategi og initiativer.
- Det er endnu ikke klart hvem der bliver påvirket og hvad effekten bliver af NIS2.
- Sektoren har lige skrevet under på aftalen omkring platformen til 3.2 og der vil være en stor indsats for at få hele sektoren på henover de næste år.
- Styregruppen er ved at revidere og gøre den nye cyber- og informationssikkerhedsstrategi klar til 2023.

https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/

Spørgsmål?

Søren Bank Greenfield

SBGR@sundhedsdata.dk

SUNDHEDSDATA-
STYRELSEN

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

T: +45 7221 6800
E: kontakt@sundshedsdata.dk
W: sundhedsdata.dk

Kontakt

DCIS Sund

DCISSUND@sundhedsdata.dk

DCISSund på Twitter
@dcissund

DCISSund information
https://sundhedsdatastyrelsen.dk/informationssikkerhed